UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

Tiffany Roper and Heidi Emmerling, individually and on behalf of all others similarly situated *Plaintiffs*, v. Rise Interactive Media & Analytics, LLC, *Defendant*.	No. 23 CV 1836 Judge Lindsay C. Jenkins

MEMORANDUM OPINION AND ORDER

Tiffany Roper and Heidi Emmerling ("Roper", "Emmerling", collectively, "Plaintiffs"), bring this putative class action against Rise Interactive Media & Analytics, LLC ("Rise" or "Defendant") based on an alleged data breach incident at Rise that exposed Plaintiffs' sensitive personal information ("SPI") to unknown third parties. Before the Court is Defendant's motion to dismiss Plaintiffs' First Amended Complaint for lack of subject matter jurisdiction under Rule 12(b)(1), and for failure to state a claim under Rule 12(b)(6). [Dkt. 16.] Defendant's motion is denied in part and granted in part.

I. Background

The following factual allegations are taken from Plaintiffs' First Amended Complaint and are accepted as true for the purposes of deciding the motion to dismiss. *Smith v. First Hosp. Lab'ys, Inc.*, 77 F.4th 603, 607 (7th Cir. 2023). Plaintiffs are customers of Edgepark Medical Supplies ("Edgepark"), a company that ships medical supplies directly to consumers. *See* [Dkt. 14 ¶¶ 1-2, 18-19.] To receive the medical

supplies, Plaintiffs provide Edgepark with a substantial amount of personal information. This includes, their name, age, date of birth, home address, telephone number, email address, government ID, social security number, credit card, bank account number, health insurance, medical diagnoses, and medical history. [*Id.* ¶¶ 3, 18.]

Defendant Rise "is a digital marketing firm that provides digital marketing [services] for various companies", including Edgepark. [*Id.* ¶¶ 1, 16.] Unbeknownst to Plaintiffs, and in an alleged violation of Edgepark policy, Edgepark sent Rise some of its customers' information, including sensitive health-related data. [*Id.* ¶ 17, 20, 28-31.]

While in possession of Plaintiffs' data, Rise experienced a data breach incident on November 14, 2022. [*Id.* ¶ 19.] Rise learned that hackers potentially stole Edgepark's customers' information on December 2, 2022, and alerted Edgepark to this three days later on December 5, 2022. [*Id.*]; [Dkt. 16 Ex. A.][1] On or about February 10, 2023, Edgepark began informing its customers that Rise had experienced a "data security incident within its systems on November 14, 2022" and that certain Edgepark customer "files may have been accessed or acquired as a result of this incident." [*Id.*] This same communication alerted the recipients that the perpetrators of the data breach may now have access to their "name, email address,

[1] The hyperlinks in Plaintiffs' First Amended Complaint at footnotes 2 and 6 do not function, but Exhibit A attached to Defendant's motion to dismiss provides the same information. Because Plaintiffs rely on this document in their pleading, the Court may consider it at the motion to dismiss stage without converting it into a motion for summary judgment. *Wright v. Associated Ins. Companies In.*, 29 F.3d 1244, 1248 (7th Cir. 1994).

phone number, provider information, diagnosis, expected delivery date and health insurance information", but that their "Social Security number, financial account information, and payment card information were **not** involved in this incident." [Dkt. 14 ¶ 21]; [Dkt. 16 Ex. A.] Defendant Rise also communicated with Edgepark's customers directly to confirm that their personal information was taken as part of the data breach. [Dkt.14 ¶¶ 54, 60.]

Plaintiff Roper is a South Carolina resident whose personal information was wrongly accessed during the data breach. [*Id.* ¶ 13.] In either late 2022 or early 2023, Roper's health insurance provider informed her that someone had attempted to use her health insurance to fill a prescription. [*Id.* ¶¶ 55, 56.] Roper has spent approximately 15 hours of her time trying to mitigate fallout from the breach, and has experienced anxiety and concern for the loss of her privacy. [*Id.* ¶¶ 57-58.]

Plaintiff Emmerling is an Indiana resident whose information was also impacted during the data breach. [*Id.* ¶ 14.] In February 2023, someone unsuccessfully attempted to open a bank account in Emmerling's name. [*Id.* ¶ 61.] Emmerling has spent roughly 20 hours trying to contain the breach, and like Plaintiff Roper, has experienced anxiety and concerns over her privacy. [*Id.* ¶¶ 62-64.]

Plaintiffs have filed this putative class action against Rise, seeking to represent a Nationwide Class of all United Staes residents, as well as a Subclass of residents from South Carolina, whose personal information was wrongfully accessed during the data breach. [*Id.* ¶¶ 66-67.] Plaintiffs bring claims for negligence (Count One), unjust enrichment (Count Two), and intrusion upon seclusion (Count Three),

alleging that they have been injured through the diminished value of their sensitive personal information ("SPI"), incurred expenses and lost time associated with mitigating harm from the breach, and the continued future risk of misuse of their SPI. [*Id.* ¶ 9.] Plaintiff Roper, on behalf of herself and the Subclass, also brings a claim under South Carolina's Data Breach Notification Act, S.C. Code § 39-1-90 *et seq.* ("SCDBNA"), arguing that she was harmed by Rise's failure to timely notify her of the breach (Count Four). Rise moves to dismiss Plaintiffs' First Amended Complaint in its entirety under Federal Rule of Civil Procedure 12(b)(1) and (6), arguing that Plaintiffs have failed to demonstrate Article III standing, and that their claims fail on the merits.

II. Legal Standards

A motion to dismiss pursuant to Rule 12(b)(1) challenges the Court's subject-matter jurisdiction, while a motion to dismiss under Rule 12(b)(6) tests the legal sufficiency of the plaintiff's claims. In both cases, the Court takes well-pleaded factual allegations as true and draws reasonable inferences in favor of the plaintiff. *Choice v. Kohn L. Firm, S.C.*, 77 F.4th 636, 638 (7th Cir. 2023); *Reardon v. Danley*, 74 F.4th 825, 826-27 (7th Cir. 2023). "To survive a motion to dismiss under Rule 12(b)(6), plaintiff's complaint must allege facts which, when taken as true, plausibly suggest that the plaintiff has a right to relief, raising that possibility above a speculative level." *Cochran v. Ill. State Toll Highway Auth.*, 828 F.3d 597, 599 (7th Cir. 2016) (cleaned up).

III. Analysis

Defendant's motion argues that Plaintiffs lack standing because they did not allege they suffered an injury in fact that is fairly traceable to Defendant's conduct under Rule 12(b)(1), but that even if they did, dismissal is still warranted under Rule 12(b)(6) because Plaintiffs have not adequately pled any of their four claims. The Court addresses these arguments in turn.

a. Standing under Rule 12(b)(1)

Defendant asserts that Plaintiffs do not have standing under Article III to bring this suit because they have not suffered an injury in fact, and any injury they may have suffered is not fairly traceable to Defendant's conduct. [Dkt. 16 at 5-6.]

The doctrine of "standing is an essential and unchanging part of the case-or-controversy requirement." *Lujan v. Defs. of Wildlife*, 112 S. Ct. 2130, 2136 (1992). It requires that the plaintiff demonstrate that he has a "personal stake in the case" sufficient to justify the exercise of federal judicial power. *TransUnion v. Ramirez*, 141 S. Ct. 2190, 2203 (2021). To establish standing, "a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief." *Id.* In a putative class action, all named plaintiffs must demonstrate "that they personally have been injured, not that injury has been suffered by other, unidentified members of the class." *Warth v. Seldin*, 95 S. Ct. 2197, 2208 (1975).

Defendant's standing argument focuses on Plaintiffs' failure to plead an injury in fact, [Dkt. 16 at 5-6], which demands that injuries are both concrete, and actual or imminent. *Ewing v. MED-1-Sols., LLC*, 24 F.4th 1146, 1151 (7th Cir. 2022). A concrete injury can be intangible, but must be "real" rather than "abstract." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). To determine whether an intangible harm is a concrete injury in fact, courts consider "whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts" and Congress's judgment in proscribing intangible harms via statute. *Id.* at 1549. The imminent requirement seeks to prohibit speculative injuries that have only a mere possibility of occurring. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013). If future harm is "certainly impending" then it is imminent. *Id.*

Plaintiffs offer two main theories to establish that they suffered an injury in fact. First, Plaintiffs argue that the mere theft of their SPI, which includes sensitive health information such as medical diagnoses, is sufficient to confer standing. [Dkt. 21 at 3-4.] Second, Plaintiffs point to the time and money they spent responding to the fraudulent attempts to use their SPI, as evidence of a concrete injury. [*Id.*] Because Plaintiffs have a right to privacy in the stolen health information, both are cognizable injuries in fact.

Along with basic demographic information, Plaintiffs' healthcare provider, medical diagnoses, and health insurance information was compromised in the data breach. [Dkt. 14 ¶ 3.] Plaintiffs' primary argument is that the disclosure of this

information constitutes a cognizable injury under Article III. [Dkt. 21 at 2.] Loss of privacy through the disclosure of private information is an intangible harm, but one that courts routinely recognize as concrete given their "close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts." *TransUnion*, 141 S. Ct. 2190 at 2204 (common intangible harms include "disclosure of private information"); *see also Lueck v. Bureaus, Inc.*, 2021 WL 4264368, at *4 (N.D. Ill. Sept. 20, 2021) ("[c]ertainly, a disclosure of private information is a concrete, albeit intangible, harm") (citations omitted); *Dixon v. Wash. & Jane Smith Cmty.-Beverly*, 2018 WL 2445292, at *10 (N.D. Ill. May 31, 2018) ("where privacy rights are concerned, the dissemination to a third party of information in which a person has a right to privacy is a sufficiently concrete injury for standing purposes.")

The question thus becomes whether Plaintiffs had a right to privacy in the stolen information. Said differently, whether the information taken in the data breach is sufficiently "private" to constitute a "common-law analogue for Plaintiffs' alleged harm." *Florence v. Order Express, Inc.*, 2023 WL 3602248, at *5 (N.D. Ill. May 23, 2023). Disclosure of private information is "one of four theories of wrongdoing under the umbrella of the tort of invasion of privacy", which "imposes liability where a defendant gives publicity to a matter concerning the private life of another, where the matter publicized is of a kind that would be highly offensive to a reasonable person, and is not of legitimate concern to the public." *Id.* at *4-5. That standard is met here.

Plaintiffs allege that Defendant caused their sensitive health information, including medical diagnoses, to be improperly accessed and publicized to an unknown number of hackers, who can then sell that information. [Dkt. 14 ¶ 48.] There is no doubt that a reasonable person would find the publication of this information to be highly offensive. *Thakkar v. Ocwen Loan Servicing*, 2019 WL 2161544, at *13 (N.D. Ill. May 17, 2019) ("facts regarding a person's financial or medical life *are* inherently private") (emphasis in original). More offensive still, hackers have already allegedly used Plaintiff Roper's diagnosis to fraudulently fill a prescription. *See Florence*, 2023 WL 3602248, at *5 ("The resulting likelihood of fraud or identity theft makes the exposure of Plaintiff's private information even more offensive"). Nor can it be said that the public has any interest in Plaintiffs' private medical history or diagnoses.

Defendant fails to meaningfully address the fact that Plaintiffs' sensitive health information was stolen in the data breach. [Dkt. 16 at 5-6; *compare* Dkt. 22 at 1-2.] Instead, Defendant argues that because Plaintiffs' financial information (e.g., SSN, credit card, bank account) was not compromised that Plaintiffs have not suffered an injury in fact. [Dkt. 16 at 5.] But this misses the mark—the theft of financial information is not required to satisfy the injury in fact requirement in a data breach case where the stolen information is sufficiently sensitive to give plaintiff a legitimate privacy interest in the stolen information. *See Florence*, 2023 WL 3602248, at *4-5; *Dixon*, 2018 WL 2445292, at *10.

The *Dixon* case cited by Plaintiffs illuminates this point. The plaintiff in *Dixon* argued that the defendant violated her right to privacy in her biometric information

by disclosing it without her authorization to a third party. *Dixon*, 2018 WL 2445292, at *9. Plaintiff did not allege that any of her financial information was disclosed. The court held that the plaintiff adequately alleged an injury in fact because "[o]btaining or disclosing a person's biometric identifiers or information without her consent or knowledge necessarily violates that person's right to privacy in her biometric information." *Id.* Defendant's response to *Dixon* is that there is a salient difference between the "highly sensitive biometric information" (i.e., fingerprints) in *Dixon* and the health information misappropriated here. [Dkt. 22 at 2.] But Defendant does not articulate the difference, and the Court disagrees. The medical diagnoses and health insurance information compromised in this case is, at minimum, equally sensitive to the biometric information in *Dixon*. *Thakkar*, 2019 WL 2161544, at *13. Plaintiffs have therefore satisfied the injury-in-fact requirement for standing.

A corollary to the Court's finding that the information stolen here is sufficiently sensitive to confer an injury in fact is that Plaintiffs' time spent monitoring and mitigating the harm from the breach is a separate injury in fact. *See Florence*, 2023 WL 3602248, at *6 (monitoring and mitigation costs are concrete and imminent injuries in fact when sensitive information has been misappropriated); *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 692 (7th Cir. 2015) (holding that plaintiff's "lost time and money resolving fraudulent charges" and "lost time and money protecting themselves against future identity theft" are concrete injuries in fact); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 965 (7th Cir. 2016) (where data breach of plaintiff's sensitive information had already occurred,

plaintiff's time spent monitoring constitutes an injury in fact); *cf. Kim v. McDonald's USA, LLC*, 2022 WL 4482826 (N.D. Ill. Sept. 27, 2022) (time spent monitoring non-sensitive personal information is not a cognizable injury in fact).

Defendant also argues that Plaintiffs have failed to allege that their injury is "fairly traceable" to Defendant's conduct. [Dkt. 16 at 6.] According to Defendant, neither Plaintiff has alleged that the data breach is connected to the alleged harm they suffered. *Id.* But that is precisely what Plaintiffs allege. Plaintiff Roper alleges that within two months of the data breach (and before Defendant or Edgepark notified her of the breach), an unknown third party attempted to use her health insurance information to fraudulently fill a prescription. [Dkt. 14 ¶ 54.] Likewise, Plaintiff Emmerling alleges that within three months of the breach, an unknown party attempted to use her personal information to open a bank account. [Dkt. 14 ¶ 61.] These allegations are sufficient at the pleading stage to satisfy the fairly traceable requirement for standing. *See Remijas*, 794 F.3d 688 at 698 (finding it "plausible for pleading purposes" where plaintiff alleged defendant's data breach caused their harm when personal information was misused in close temporal proximity to defendant's breach.) The Court therefore finds that Plaintiffs have satisfied their standing requirements, and Defendant's motion to dismiss under Rule 12(b)(1) is denied.[2]

[2] The Court's conclusion that Plaintiffs have established a concrete standing injury by alleging theft of SPI and by alleging they spent time and money responding to fraudulent attempts to use their SPI, both of which are fairly traceable to Defendant's conduct, distinguishes this case from *Baysal v. Midvale Indem. Co.*, 78 F.4th 976, 977 (7th Cir. 2023). *Baysal* acknowledged that individuals injured by leaked or hacked data can have standing

b. Failure to state a claim under Rule 12(b)(6)

The Court now turns to whether Plaintiffs have adequately pled claims for negligence, unjust enrichment, intrusion upon seclusion, and a claim under the SCDBNA for Plaintiff Roper, each of which Defendant has moved to dismiss pursuant to Rule 12(b)(6).

The Court applies Illinois law to the first three claims. While the Parties' briefing discusses potential choice-of-law issues, all agree that Illinois law governs, so the Court will apply forum law. *See Sosa v. Onfido, Inc.*, 8 F.4th 631, 637 (7th Cir. 2021) ("Under Illinois choice-of-law rules, forum law is applied unless an actual conflict with another state's law is shown, or the parties agree that forum law does not apply") (citations omitted). The Court will analyze each claim in turn.

i. Negligence

Defendant's motion to dismiss provides three bases for why Plaintiffs' negligence claim should be dismissed: (1) Defendant did not have a duty to protect Plaintiffs' personal information; (2) Illinois's economic-loss doctrine bars the negligence claim; and (3) Plaintiffs' have failed to allege damages under Illinois law. [Dkt. 16 at 7-9]. Because the Court concludes that Defendant did not owe Plaintiffs—neither of whom are Illinois residents—a duty to safeguard their personal information, it does not reach the issues of the economic loss or damages.

---

so long as they can show concrete injury traceable to the disclosure. But it reiterated that "worry and anxiety are not the kind of concrete injury essential to standing," while noting that plaintiffs in that case had not adequately alleged that any expenses incurred were fairly traceable to the disclosure of drivers'-license numbers. *Id.*

Under Illinois law, a cause of action for negligence requires the plaintiff to "plead that the defendant owed a duty of care to the plaintiff, that the defendant breached that duty, and that the breach was the proximate cause of the plaintiff's injuries." *Cowper v. Nyberg*, 2015 IL 117811, ¶ 13. In deciding whether a legal duty exists at common law, courts look to "the reasonable foreseeability of the injury, the likelihood of the injury, the magnitude of the burden of guarding against the injury, and the consequences of placing that burden on the defendant." *Bogenberger v. Pi Kappa Alpha Corp., Inc.*, 2018 IL 120951, ¶ 46. Where a common law duty does not exist, "a duty may also be created by statute or ordinance." *Dixon*, 2018 WL 2445292, at *12.

Based on an intermediate Illinois Appellate Court decision, the Seventh Circuit has held that Illinois does not have a "common law data security duty." *Cmty. Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 816 (7th Cir. 2018); *Cooney v. Chicago Pub. Sch.* 943 N.E.2d 23, 28-29 (1st Dist. 2010) (rejecting argument that Illinois should create a "new common law duty to safeguard information"). The *Cooney* court recognized the "importance of protecting" sensitive information but held "that the creation of a new legal duty beyond legislative requirements already in place" was beyond the scope of the judiciary. *Id.* at 29. At the time *Cooney* was decided, the Illinois Personal Information Protection Act ("PIPA") required a data collector to notify an aggrieved party when a data breach incident occurred but did not require the data collector to employ reasonable security measures. *Id.* at 28.

Defendant cites to these cases approvingly to argue that it had no duty to protect Plaintiffs' data from hackers. [Dkt. 16 at 7].

In response, Plaintiffs assert that Defendant had a statutory duty to protect their sensitive information in November 2022 (when the data breach occurred) because the Illinois legislature amended PIPA in 2017 to require data collectors to "implement and maintain reasonable security measures" to protect "records that contain personal information concerning an Illinois resident." 815 ILCS 530/45; [Dkt. 21 at 5.] Plaintiffs argue that the creation of this duty is consistent with *Cooney* because *Cooney* only rejected broadening the common-law duty beyond what was statutorily prescribed. [Dkt. 21 at 5.] Courts applying Illinois law since the PIPA amendment have found that a negligence cause of action can proceed based on a defendant's alleged failure to adequately protect personal information. *See In re Arthur J. Gallagher*, 631 F. Supp.3d 573, 590 (N.D. Ill. 2022); *see also Dixon*, 2018 WL 2445292, at *12-13 (allowing negligence claim to proceed for failure to protect biometric information as statutorily required under Illinois's Biometric Information Privacy Act).

The dispositive problem for Plaintiffs is that they are not Illinois residents. Consequently, the protections created in PIPA, and the concomitant duties placed upon data collectors, do not apply.[3] [Dkt. 22 at 3.] The relevant PIPA provision is as follows:

[3] Defendant argues that it does not qualify as a data collector under PIPA. [Dkt. 26 at 3.] The Court does not take a position on the issue but *assumes arguendo* Defendant does so qualify for purposes of this argument.

> A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

815 ILCS 530/45(a). As the plain language suggests, Courts applying this provision have found that a data collector's duty to protect information only applies to Illinois residents. *McGlenn v. Driveline Retail Merch., Inc.*, 2021 WL 4301476, at *7 (C.D. Ill. Sept. 21, 2021) (defendant's "duty under this provision is expressly limited to Illinois residents" and defendant "did not owe a duty under Illinois law to safeguard" non-Illinois resident's personal information); *USAA Fed. Sav. Bank v. PLS Fin. Servs.*, 260 F. Supp. 3d 965, 971-972 (N.D. Ill. 2017). Plaintiffs do not rely on any other statutory authority that would create a duty for Defendant to protect their personal information, and no common-law duty exists, so Plaintiffs' negligence claim is dismissed.

ii. Unjust Enrichment

Next is Plaintiffs' claim for unjust enrichment, based on the theory that Defendant has retained the benefit of Plaintiffs' SPI, which Defendant allegedly used to "facilitate [Defendant's] core functions" and "pay for or recoup the administrative costs of reasonable data privacy and security practices and procedures." [Dkt. 14 at 21.]

"To state a cause of action based on a theory of unjust enrichment, a plaintiff must allege that the defendant has unjustly retained a benefit to the plaintiff's detriment, and that defendant's retention of the benefit violates the fundamental

principles of justice, equity, and good conscience." *Flores v. Aon Corp.*, 2023 WL 6333957, at *7 (Ill. Ct. App. Sept. 29, 2023). "Unjust enrichment is not an independent cause of action." *Id.*

Plaintiffs' unjust enrichment claim fails because they have failed to plausibly allege that they conferred a benefit on Defendant, or that Defendant retained this benefit. In *In re Arthur J. Gallagher*, plaintiffs alleged that a defendant insurance broker injured them by "failing to secure and safeguard their personally identifiable information and/or protected health information" in a third-party data breach. *In re Arthur J. Gallagher*, 631 F. Supp.3d at 581. Plaintiffs argued that defendant retained the monetary value of plaintiffs' personal information, but the court rejected that argument, finding the "third-party hackers, not Defendants, are the ones who benefitted from the Data Breach" and that courts "routinely reject[] the proposition that an individual's personal identifying information has an independent monetary value." *Id.* at 591–92; *Flores*, 2023 WL 6333957 at *7. The same reasoning applies here. Defendant's alleged retention of Plaintiffs' SPI does not confer a benefit on Defendant's as that term is understood for purposes of unjust enrichment. Plaintiff's unjust enrichment claim is dismissed.

iii. Intrusion Upon Seclusion

Plaintiff also brings a claim for intrusion upon seclusion, [Dkt. 14 at 22-23], although it is not entirely clear to the Court whether this claim is based on Defendant's initial obtainment of Plaintiffs' SPI from Edgepark, or the data breach

itself. [Dkt. 14 ¶ 103; *compare* Dkt. 14 ¶¶ 104-106]; *see also* [Dkt. 21 at 11-12.] The Court concludes that the claim fails under either theory.[4]

"Under Illinois law, a claim of intrusion upon seclusion requires the following elements: (1) an unauthorized intrusion or prying into the plaintiff's seclusion; (2) an intrusion that is highly offensive or objectionable to a reasonable person; (3) that the matter upon which the intrusion occurs is private; and (4) the intrusion causes anguish and suffering." *In re Arthur J. Gallagher*, 631. F.Supp.3d at 598. "The nature of this tort depends upon some type of highly offensive prying into the physical boundaries or affairs of another person." *Bonilla v. Ancestry.com Operations Inc.*, 574 F.Supp.3d 582, 596 (N.D. Ill. 2021). The Supreme Court of Illinois has approvingly cited to the Restatement (Second) of Torts' definition of the tort: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." *Lawlor v. N. Am. Corp. of Ill.*, 2012 IL 112530, ¶ 33. The act of prying itself must cause the harm in an intrusion upon seclusion claim, and plaintiffs who allege that the publication of private information caused their harm "plead[s] themselves out of court." *Angelo v. Moriarty*, 2016 WL 640525, at *5 (N.D. Ill. Feb. 18, 2016).

To the extent Plaintiffs' intrusion upon seclusion claim is based on the data breach, their claim fails because they have not alleged that Defendant made an

[4] A third potential interpretation is that Plaintiffs seek to use a combination of Defendant's acquisition of Plaintiffs' SPI and the data breach to state their claim. But Plaintiffs cite to no authority in support of the notion that a single claim for intrusion upon seclusion can be based on two independent intrusions.

intentional intrusion, and the intrusion itself, rather than the publication of their private information, caused their damages. To address the latter point first, Plaintiffs have "pleaded themselves out of court" by arguing that they "readily satisfy" the damages element of the intrusion claim by alleging they have "experienced anxiety and increased concerns for the loss of [their] privacy *since the time of the breach*." [Dkt. 14 ¶¶ 58, 64]; [Dkt. 21 at 11.] (emphasis added). Alleged damages in an intrusion claim "must flow from the *intrusion*, not the later publication" of their private information. *Bonilla v. Ancestry.com Operations Inc.*, 574 F.Supp.3d 582, 597 (N.D. Ill. 2021); *Angelo*, 2016 WL 640525, at *5 (dismissing intrusion upon seclusion claim where plaintiff alleged his injury stemmed from publication of private information.) Plaintiffs here allege that their injury is the impending threat of the publication of their private information. [Dkt. 14 ¶¶ 58, 64]; *see also* [*id.* ¶ 108] ("SPI of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.") That allegation does not adequately plead injury for an intrusion upon seclusion claim.

Even if Plaintiffs had properly alleged that they were injured by the hackers' intrusion into their private information, the claim would still fail because they do not allege that Defendant made an intentional intrusion. The court in *White* analyzed an intrusion upon seclusion claim stemming from a data breach and held dismissal was proper because "[n]othing in plaintiff's complaint allows the court to reasonably infer that [defendant] intentionally shared his information with third parties." *White v.*

Citywide Title Corp., 2018 WL 5013571, at *3 (N.D. Ill. Oct. 16, 2018). The same logic applies here. Plaintiffs do not allege that Defendant intentionally provided their private information to the hackers; indeed, they allege the opposite—Defendant negligently allowed the hackers to access their data. In other words, it was the hackers, not Defendant, who made the unauthorized intrusion.

Plaintiffs' claim likewise fails to the extent it is based on Defendant's acquisition of their private information from Edgepark because they do not allege that Defendant's mere possession of their SPI caused them damages.[5] Plaintiffs say that it is "unclear" to them how Defendant received their SPI, and why it was necessary for Defendant to have access to their SPI to perform their digital marketing duties for Edgepark. [Dkt. 14 ¶ 17.] But Plaintiffs do not allege that Defendant's mere possession of their SPI—absent and prior to any data breach—caused them harm.

Accordingly, whether the Court interprets Plaintiffs' claim for intrusion upon seclusion to be based on the data breach or Rise's initial acquisition of Plaintiffs' SPI, the claim fails. Accordingly, all claims brought by Plaintiff Emmerling are dismissed.

iv. South Carolina Data Breach Notification Act

Finally, Defendant moves to dismiss Plaintiff Roper's SCDBNA claim because she has failed to allege that Defendant owns or licenses data as is required under S.C. Code § 39-1-90(A). [Dkt. 16 at 15.] Plaintiff argues in response that "further discovery is needed" to determine whether Defendant owns or licenses data, but that in any event Plaintiff has adequately pled a claim under S.C. Code § 39-1-90(B), which

[5] The Court does not take a position on whether Plaintiffs have satisfied the other elements of the claim.

applies to those who merely maintain personally identifying information. [Dkt. 21 at 13.] Defendant disputes that Plaintiff has alleged a violation of that section. [Dkt. 22 at 7.]

The SCDBNA places similar, but different data breach reporting obligations on those who either "own or license" or "maintain" personal identifying information. S.C. Code § 39-1-90(A)-(B). Those that own or license data "shall disclose a breach of the security of the system following discovery or notification of the breach" to a South Carolina resident "in the most expedient time possible and without unreasonable delay." *Id.* at (A). Conversely, the entities that maintain personal identifying information are required to "notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person." *Id.* at (B).

Plaintiff has failed to adequately allege facts that allow the Court to infer that Defendant owns or licenses Plaintiffs' SPI under subsection A. The First Amended Complaint alleges that Edgepark provided Defendant with Plaintiffs' SPI to facilitate Defendant's digital marketing for Edgepark. *See* [Dkt. 14 ¶¶ 16-17.] That allegation does not support a conclusion that Defendant owns or licenses the SPI. Plaintiff's sole argument in support of its subsection A claim is that dismissal is "premature" because it is "impossible to determine" whether Rise licensed the data from Edgepark based on the facts known to her. [Dkt. 21 at 13.] This does not satisfy Plaintiff's pleading burden. *Choice*, 77 F.4th 636 at 638.

The Parties disagree as to whether Plaintiff also brings a claim under subsection B of the statute. In support of its argument, Defendant relies on *In re Blackbaud, Inc.*, where the court held that the two subsections "provide for separate claims", and so a plaintiff had to identify which subsection provided the basis for the claim. *In re Blackbaud, Inc.*, 2021 WL 3568394, at *16 (D.S.C. Aug. 12, 2021). But the plaintiff in that case "explicitly pursue[d] claims under S.C. Code Ann. § 39-l-90(A) and fail[ed] to even reference S.C. Code Ann. § 39-l-90(B)" in the operative pleading, so the court held the plaintiff could not substitute one subsection for the other. *Id.*

Plaintiff's allegations here are not so cut-and-dried. Plaintiff brings her claim under the SCDBNA generally, and references both subsections in her allegations. [Dkt. 14 at 23-24.] While the basis for Plaintiffs' claim is ambiguous, the Court concludes that Plaintiff would not have included Paragraph 114 in the First Amended Complaint had she not intended to bring a claim under that subsection.

Plaintiff has properly alleged a claim under subsection B. Plaintiff—who undoubtedly "owns" her SPI and is therefore owed "immediate" notice of a data breach under subsection B—alleges that Defendant learned that Plaintiff's SPI may have been compromised on December 2, 2022, but did not inform Plaintiff of the potential breach until February 15, 2023. [Dkt. 14 ¶ 54]; [Dkt. 16 Ex. A.] Defendant does not suggest that the two-month delay in notifying Plaintiff qualifies as immediate notice. Rather, it argues that it satisfied the immediate notification obligation by informing Edgepark of the breach on December 5, 2022. [Dkt. 22 at 7.]

Even if the Court were inclined to accept the argument that notice to Edgepark was sufficient, it declines to hold now as a matter of law that notification within 72 hours qualifies as "immediately". Plaintiff has plausibly alleged a claim under (B).

IV. Conclusion

Defendant's motion to dismiss is denied in part and granted in part. Plaintiffs are ordinarily given at least one opportunity to amend a complaint "[u]nless it is *certain* from the face of the complaint that any amendment would be futile." *Runnion ex rel. Runnion v. Girl Scouts of Greater Chi. & Nw. Ind.*, 786 F.3d 510, 520 (7th Cir. 2015) (emphasis in original). The Court therefore dismisses the claims as follows:

Plaintiffs' negligence claim (Count One) is dismissed with prejudice to the extent the claim relies on PIPA to allege Defendant had a duty to safeguard their SPI, but is otherwise dismissed without prejudice. Plaintiffs' unjust enrichment claim (Count Two) is dismissed with prejudice. Plaintiffs' intrusion upon seclusion claim (Count Three) is dismissed without prejudice. Plaintiff Roper's SCDBNA claim (Count Four) brought under § 39-1-90(A) is dismissed without prejudice.

Plaintiffs may file a second amended complaint no later than November 28, 2023, if they can do so consistent with this opinion and Rule 11. Otherwise, the case will proceed only as to Plaintiff Roper on Count Four under S.C. Code § 39-1-90(B).

Enter: 23-cv-1836
Date: November 9, 2023

Lindsay C. Jenkins
United States District Judge